

ISSN 2518-1483 (Online),
ISSN 2224-5227 (Print)

2017 • 4

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

БАЯНДАМАЛАРЫ

ДОКЛАДЫ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

REPORTS

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

ЖУРНАЛ 1944 ЖЫЛДАН ШЫҒА БАСТАҒАН
ЖУРНАЛ ИЗДАЕТСЯ С 1944 г.
PUBLISHED SINCE 1944



Бас редакторы
х.ғ.д., проф., ҚР ҰҒА академигі **М.Ж. Жұрынов**

Редакция алқасы:

Адекенов С.М. проф., академик (Қазақстан) (бас ред. орынбасары)
Боос Э.Г. проф., академик (Қазақстан)
Величкин В.И. проф., корр.-мүшесі (Ресей)
Вольдемар Вуйцик проф. (Польша)
Гончарук В.В. проф., академик (Украина)
Гордиенко А.И. проф., академик (Белорус)
Дука Г. проф., академик (Молдова)
Илолов М.И. проф., академик (Тәжікстан),
Леска Богуслава проф. (Польша),
Локшин В.Н. проф. чл.-корр. (Қазақстан)
Нараев В.Н. проф. (Ресей)
Неклюдов И.М. проф., академик (Украина)
Нур Изура Удзир проф. (Малайзия)
Перни Стефано проф. (Ұлыбритания)
Потапов В.А. проф. (Украина)
Прокопович Полина проф. (Ұлыбритания)
Омбаев А.М. проф. (Қазақстан)
Өтелбаев М.О. проф., академик (Қазақстан)
Садыбеков М.А. проф., корр.-мүшесі (Қазақстан)
Сатаев М.И. проф., корр.-мүшесі (Қазақстан)
Северский И.В. проф., академик (Қазақстан)
Сикорски Марек проф., (Польша)
Рамазанов Т.С. проф., академик (Қазақстан)
Такибаев Н.Ж. проф., академик (Қазақстан), бас ред. орынбасары
Харин С.Н. проф., академик (Қазақстан)
Чечин Л.М. проф., корр.-мүшесі (Қазақстан)
Харун Парлар проф. (Германия)
Энджун Гао проф. (Қытай)
Эркебаев А.Э. проф., академик (Қырғыстан)

«Қазақстан Республикасы Ұлттық ғылым академиясының баяндамалары»
ISSN 2518-1483 (Online),
ISSN 2224-5227 (Print)

Меншіктенуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» Республикалық қоғамдық бірлестігі (Алматы қ.)
Қазақстан республикасының Мәдениет пен ақпарат министрлігінің Ақпарат және мұрағат комитетінде 01.06.2006 ж.
берілген №5540-Ж мерзімдік басылым тіркеуіне қойылу туралы куәлік

Мерзімділігі: жылына 6 рет.

Тиражы: 2000 дана.

Редакцияның мекенжайы: 050010, Алматы қ., Шевченко көш., 28, 219 бөл., 220, тел.: 272-13-19, 272-13-18,
http://nauka-nanrk.kz_reports-science.kz

© Қазақстан Республикасының Ұлттық ғылым академиясы, 2017

Типографияның мекенжайы: «Аруна» ЖК, Алматы қ., Муратбаева көш., 75.

Главный редактор
д.х.н., проф., академик НАН РК **М. Ж. Журинов**

Редакционная коллегия:

Адекенов С.М. проф., академик (Казахстан) (зам. гл. ред.)
Боос Э.Г. проф., академик (Казахстан)
Величкин В.И. проф., чл.-корр. (Россия)
Вольдемар Вуйцик проф. (Польша)
Гончарук В.В. проф., академик (Украина)
Гордиенко А.И. проф., академик (Беларусь)
Дука Г. проф., академик (Молдова)
Илолов М.И. проф., академик (Таджикистан),
Леска Богуслава проф. (Польша),
Локшин В.Н. проф. чл.-корр. (Казахстан)
Нараев В.Н. проф. (Россия)
Неклюдов И.М. проф., академик (Украина)
Нур Изура Удзир проф. (Малайзия)
Перни Стефано проф. (Великобритания)
Потапов В.А. проф. (Украина)
Прокопович Полина проф. (Великобритания)
Омбаев А.М. проф. (Казахстан)
Отелбаев М.О. проф., академик (Казахстан)
Садыбеков М.А. проф., чл.-корр. (Казахстан)
Сатаев М.И. проф., чл.-корр. (Казахстан)
Северский И.В. проф., академик (Казахстан)
Сикорски Марек проф., (Польша)
Рамазанов Т.С. проф., академик (Казахстан)
Такибаев Н.Ж. проф., академик (Казахстан), зам. гл. ред.
Харин С.Н. проф., академик (Казахстан)
Чечин Л.М. проф., чл.-корр. (Казахстан)
Харун Парлар проф. (Германия)
Энджун Гао проф. (Китай)
Эркебаев А.Э. проф., академик (Кыргызстан)

«Доклады Национальной академии наук Республики Казахстан»

ISSN 2518-1483 (Online),

ISSN 2224-5227 (Print)

Собственник: Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы)

Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан №5540-Ж, выданное 01.06.2006 г.

Периодичность: 6 раз в год.

Тираж: 2000 экземпляров

Адрес редакции: 050010, г.Алматы, ул.Шевченко, 28, ком.218-220, тел. 272-13-19, 272-13-18

<http://nauka-nanrk.kz> reports-science.kz

©Национальная академия наук Республики Казахстан, 2017 г.

Адрес типографии: ИП «Аруна», г.Алматы, ул.Муратбаева, 75

E d i t o r i n c h i e fdoctor of chemistry, professor, academician of NAS RK **M.Zh. Zhurinov****E d i t o r i a l b o a r d :****Adekenov S.M.** prof., academician (Kazakhstan) (deputy editor in chief)**Boos E.G.** prof., academician (Kazakhstan)**Velichkin V.I.** prof., corr. member (Russia)**Voitsik Valdemar** prof. (Poland)**Goncharuk V.V.** prof., academician (Ukraine)**Gordiyenko A.I.** prof., academician (Belarus)**Duka G.** prof., academician (Moldova)**Ilov M.I.** prof., academician (Tadjikistan),**Leska Boguslava** prof. (Poland),**Lokshin V.N.** prof., corr. member. (Kazakhstan)**Narayev V.N.** prof. (Russia)**Nekludov I.M.** prof., academician (Ukraine)**Nur Izura Udzir** prof. (Malaysia)**Perni Stephano** prof. (Great Britain)**Potapov V.A.** prof. (Ukraine)**Prokopovich Polina** prof. (Great Britain)**Ombayev A.M.** prof. (Kazakhstan)**Otelbayv M.O.** prof., academician (Kazakhstan)**Sadybekov M.A.** prof., corr. member. (Kazakhstan)**Satayev M.I.** prof., corr. member. (Kazakhstan)**Severskyi I.V.** prof., academician (Kazakhstan)**Sikorski Marek** prof., (Poland)**Ramazanov T.S.** prof., academician (Kazakhstan)**Takibayev N.Zh.** prof., academician (Kazakhstan), deputy editor in chief**Kharin S.N.** prof., academician (Kazakhstan)**Chechin L.M.** prof., corr. member. (Kazakhstan)**Kharun Parlar** prof. (Germany)**Endzhun Gao** prof. (China)**Erkebayev A.Ye.** prof., academician (Kyrgyzstan)**Reports of the National Academy of Sciences of the Republic of Kazakhstan.****ISSN 2224-5227****ISSN 2518-1483 (Online),****ISSN 2224-5227 (Print)**

Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)

The certificate of registration of a periodic printed publication in the Committee of Information and Archives of the Ministry of Culture and Information of the Republic of Kazakhstan N 5540-Ж, issued 01.06.2006

Periodicity: 6 times a year

Circulation: 2000 copies

Editorial address: 28, Shevchenko str., of.219-220, Almaty, 050010, tel. 272-13-19, 272-13-18,

<http://nauka-nanrk.kz> / reports-science.kz

© National Academy of Sciences of the Republic of Kazakhstan, 2017

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

**REPORTS OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN**

ISSN 2224-5227

Volume 4, Number 314 (2017), 29 – 34

B.S. Akhmetov, T.S. Kartbayev, A.A. Doszhanovabahitzhan@rambler.ru, kartbaev_t@mail.ru, d_alia.81@mail.ru
S.D. Asfendiyarov Kazakh National Medical University, Almaty**METHODS OF COUNTERACTION TO MEANS OF BIOMETRIC-
NEURAL NETWORK PROTECTION OF INFORMATION**

Abstract. Today, it is not enough to protect the system only with the help of hardware, that is, the organizational, legal, physical and technical complex must be provided for the reliability of protection. This article discusses the methods of counteraction to means of biometric-neural network protection of information methods. Each method is considered in practice in the laboratories of the Kazakh National Research Technical University named after K.I.Satpayev and Penza State University.

Keywords: information security, biometrics, neural networks, authentication, threats, information protection.

Б.С. Ахметов, Т.С. Картбаев, А.А. Досжанова

С.Ж.Асфендияров атындағы Қазақ ұлттық медицина университеті, Алматы қ., Қазақстан

**АҚПАРАТТАРДЫ НЕЙРОЖЕЛІЛІК БИОМЕТРИЯЛЫҚ ҚОРҒАУ
ҚҰРАЛДАРЫНА ТӨНЕТІН ҚАУІПKE ҚАРСЫ ТҰРУ ӘДІСТЕРІ**

Аннотация. Бүгінгі күні техникалық құралдармен жүйені тиімді қорғау мүмкін емес яғни ұйымдастырушылық, заңдылық, физикалық және техникалық кешен қажет. Осы мақала шеңберінде ақпараттарды нейрожелілік биометриялық қорғау құралдарына төнетін қауіптерге қарсы тұру әдістері қарастырылды. Олардың әрқайсысы тәжірибеде Қ.И.Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университетінің және Пенза мемлекеттік университетінің зертханаларында қарастырылып, ұсынылып отыр.

Түйін сөздер: ақпараттық қауіпсіздік, биометрия, нейрожелі, аутентификация, қауіп, ақпаратты қорғау.

1 Кіріспе. Қарқынды келе жатқан заманауи қоғамды ақпараттандыру үрдісі мен халықтың электронды үкімет және бизнестің ON-LINE қызметтерін қолдануға белсенді өтуі, сонымен бірге, электронды қызметтер азаматтардың электрондық хабарласуын сенімді авторизациялау, ал азаматтар Интернет желісінде айналып жүретін, өз жеке ақпараттарын сенімді қорғауды қажет етуінен біздің қоғамымызда күрделі мәселе туындады. Осы мәселені шешудің ең тиімді жолдарының бірі кодты қолданушының биометриясына байланыстыру екені белгілі мәселе [1]. Бірақ, таза күйінде олар теру шабуылдарына төмен тұрақтылыққа ие болғандықтан, шектеулі қолданысқа ие [2-6].

Қазіргі кездегі қалыптасқан биометриялық куәландыру орталығының жүйесінде биометриялық шаблон қалыптастырылады. Биометриялық шаблонды шифрлауға болмайды, себебі идентификациялау жүйесі оны қолдануы қажет. Мәселені шешуге бұл әдіс биометриялық шаблондарды жоғалту қауіпі болғандықтан қатерлі, бірақ полициялық төлқұжатты-визалық тексеру және ұжымдық биометриялық жүйеге кіруді шектеу қосымшаларында қолдануға толық лайықты [7].

Алайда, қолданушы саусақ таңбасы немесе көзінің шатырша қабығы суретінің биометриялық шаблонды тек оның биометриялық картасына ғана емес, сонымен қатар, сәйкес ортақтандырылған деректер қорына да түседі. Бұл осы ұйымда жұмыс істейтін, сондай-ақ онымен белсенді әрекеттесетін сырттың адамдарының үлкен көлемдегі жасырын биометриялық ақпараттары жиналатын ұжымдық биометриялық деректер қоры болуы мүмкін. Ең көп көлемдегі жасырын биометриялық ақпарат мемлекеттік биометриялық деректер қорында жиналуы мүмкін.

Адамдардан олардың биометриясын алып, үлкен деректер қорында оларды орналастыру өте қауіпті болып есептеледі.

Биометриялық шаблондарды әшкерелеу қауіпін болдырмау үшін бір жағынан жоғары дәрежелі сенімділікпен аутентификациялауға мүмкіндік беретін, екінші жағынан адам биометриясын бақылауға және түсінуге қол жеткізбейтін ететін, жаңа биометриялық технологияларды құру қажет болды. Бұл мәселелер де, биометриялық деректерді ішінара жасырын және иесіздендіруді қамтамасыз етудің бір жолы үлкен және өте үлкен өлшемдегі нейрондық желілерді қолдану арқылы шешілді [7-11].

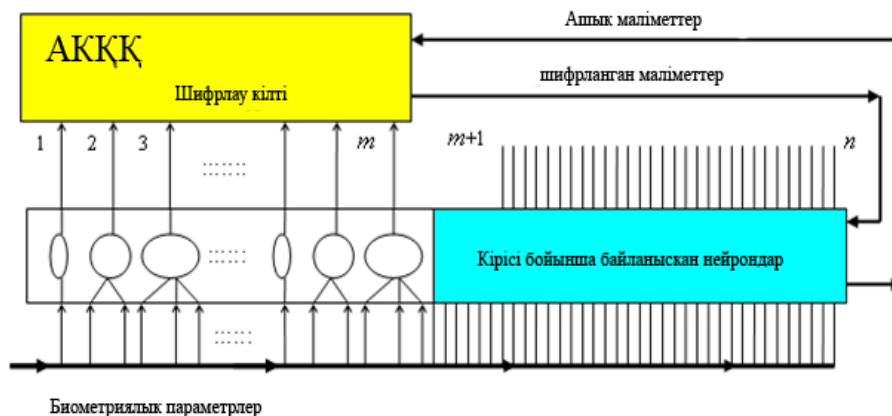
Нейрожелілік шешімнің жағымды жағы бұрын ашық түрде сақталған биометриялық шаблонның болмауы, ал оның орнына нейрожелілік биометрия-кодты түрлендіргіш пайда болды. Шын мәнінде, бұл нейрондық желі нейрондары байланысының кестесі мен «Өзім» нейрондық желісін тануға үйретілген синаптикалық байланыстар кестесі. Үйретілген нейрондық желі байланыстары кестесі мен коэффициенттер салмағы кестелері бойынша биометриялық бейнелер қорынан адамды табу техникалық жақтан өте қиын болғандығы есебінен биометрия құпиялылығы қамтамасыз етіледі. Нейрожелілік контейнерде орналастырылған биометрия құпиялылығы шифрлау қамтамасыз ететін құпиялылық деңгейімен пара-пар келеді [7, 8, 12].

Бірақ осы күнге дейін қолданылып келген бұл шешімдерге де төнетін қауіп-қатерлер табылып отыр. Яғни ұсынылып отырған мақалада, осындай қауіптерге қарсы тұру әдістері қарастырылған.

2 Жеке мәліметтерді биометриялық қорғау құралдарына төнетін қауіп және шабуылдарға қарсы тұру әдістері.

2.1 Нейрожелілік контейнердің мәліметтерін қарапайым шифрлау арқылы криптографиялық қорғау.

Ең қарапайым және түсінікті қорғау тәсілдерінің бірі – алғашқы (ашық) нейрондардың шығысымен кілттің алынуы және онда өзге нейрондардың (қорғалған) мәліметтерін шифрлау [13-15]. Бұл жағдай 2-суретте көрсетілген.



Сурет 2 – Нейрожелілік контейнер мәліметтерін саны өте көп болатын айқастырылған байланыстарды шифрлау арқылы қорғау

2-суреттен алғашқы m нейрондарының мәліметтері ашық сақталатыны, ал келесі нейрондардың мәліметтері қорғалған контейнерді даярлау кезінде m ұзындықты кілтте шифрланғаны көрініп тұр. Қорғалған контейнерді қолданғанда пайдаланушы өзінің биометриясын көрсетеді, ол ұзындығы m биометрия-кодқа түрленеді және әрі қарай осы кодта алдын шифрлаумен қорғалған келесі нейрондардың мәліметтері шифрлаудан шығарылады.

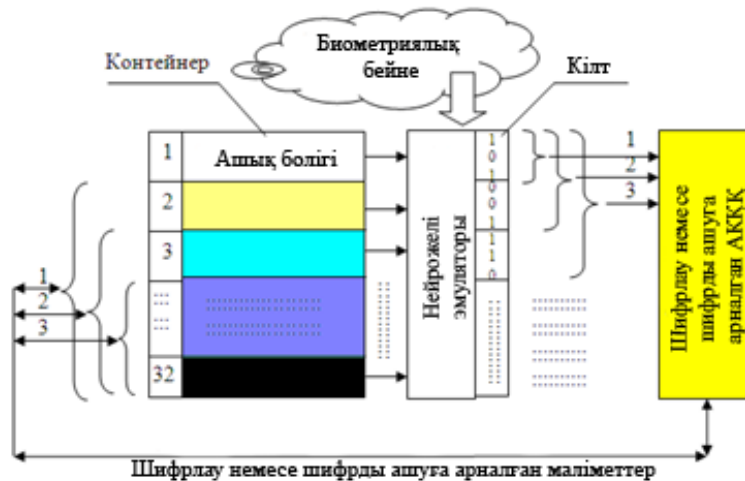
Бұл жерде әрине, m шифрлау кілті кодының ұзындығы қандай болуы тиіс деген сұрақ туындайды. Шифрлау кілтінің ұзындығы криптографиялық және биометриялық шектеулер қатарынан шығуы тиіс. Ең қарапайым нұсқасы – кілт ұзындығын теру шабуылының 3 еселік тұрақтылық көрсеткішіне пропорционалды етіп алу болып табылады (биометрия тұрақтылығы 2^{40} болғанда шифрлау 2^{120} құрауы тиіс). Басқаша айтқанда, шифрлау кілтінің ұзындығы 120 бит

болғанда, алғашқы 120 нейрон мәліметтерін ашық сақтау қажет (120 нейрон үшін салмақтар және байланыстар кестесі жалпыға қол жетімді).

0.2 бит био-параметрінің орташа ақпараттылығы кезінде әр нейронның 5 кірісі бойынша орташа алғанда 600 био-параметрлер үшін 600 кіріс шығады. Егер нейрондық желінің кіріс саны тек 480 болса, онда қалған 220 кіріс нейрондардың ашық бөліктерінде қайталанатын болады. Әр нейрон өз көршілерімен шамамен 2 кіріс арқылы байланысатын болады. Әр нейронның көршілерімен жабылатын екі кірісі Маршалко шабуылының табысты түрде ұйымдастырылуы үшін барынша жеткілікті болады.

Сондай-ақ үйретілген нейрондардың ашық мәліметтерінің ұзын серияларына разрядтардың тұрақтылығына және энтропия бақылауы арқылы «Өзім» кілттің кодын алуға шабуыл жасалуы мүмкін. Бұл шабуылдар код ұзындығын 80%-дан 90%-ға дейін қысқартуға алып келеді яғни 120 бит иллюзиялықтың (алдамшының) орнына біз 12 немесе 24 нақты биттегі шифрлауды аламыз. Осындай шифрлаудың тұрақтылығы биометриялық қорғаудың айтылған тұрақтылығынан көп есе төмен болып шығады (2^{40} -тан 2^{12} -:- 2^{24} анағұрлым кіші).

2.2 Криптографиялық кілттің өсетін ұзындығымен блоктық шифрлау арқылы нейрондарды қорғау. Бір ұзын кілтте шифрлаудың барлығына түсінікті нұсқасын жүзеге асыру биометрияға жасалатын шабуылдардың тиімділігінен мүмкін болмайды. Бұл шабуылдардың барлығы ашық нейрондардың үлкен санына жасалатын барлық интегралды шабуылдардан тиімді қорғау үшін қорғалмаған нейрондардың көп мөлшердегі шығысының болуын бақылауға қарай құрылады. Биометрияға жасалатын интегралдық шабуылдың тиімділігін төмендету үшін бір ұзын кілтті жасаудан бас тартып, арттырылатын ұзындықты кілттердің жиынтығын қолдану керек. Осындай блоктық шифрлау үлгісінің мысалы 3-суретте келтірілген [13, с. 57].



Сурет 3 – Кілт ұзындығы 3, 6, 12, 15..., 256 бит болып яғни еселеп өсетін блоктық шифрлау арқылы мәліметтерді қорғау

Барлық шағын кілттер бір-бірімен біріктіріледі және қорғалған нейрожелілік контейнерді дайындау процесінде барлық соңғы үйретілген нейрондардың мәліметтерін көп еселеп шифрлайды. Қорғалған нейрожелілік контейнерді пайдалану кезінде кері процесс жүреді, ашық нейрондардан алынған кілт барлық соңғы нейрондардың мәліметтерін ашады. Қайта қалпына келтірілетін кілттің тағы бір бөлігі ашық болады, олар біріншімен бірігеді де, келесі мәліметтерді ашады. Бұл 3-суретте бояулардың қоюлатылуымен көрсетілген. Нейрондардың ашық бөлігі боялмаған.

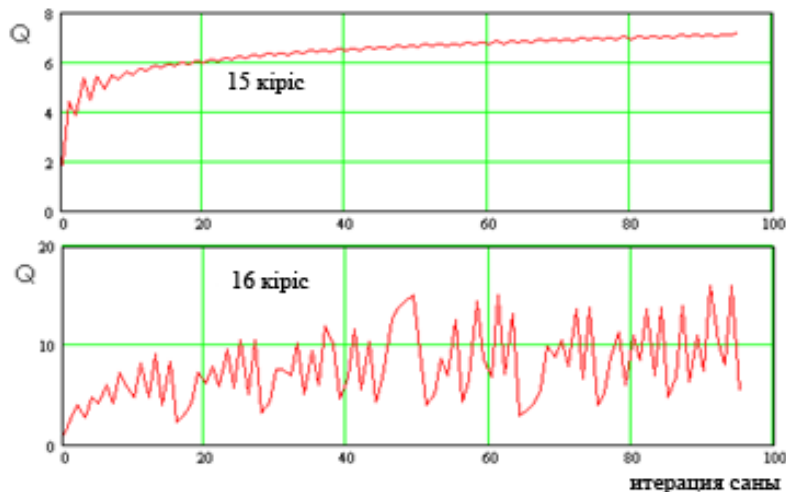
Бір ұзын кілтті ашық биометрияға бірнеше интегралдық шабуылдың болуына байланысты қолдана алмаймыз. Баяу артып отыратын кілт ұзындығы мен шифрланған мәтіннің кемитін ұзындығымен блоктық шифрлау кілтінің өсу дискретінің ұзындығын таңдау маңызды болады.

Шифрлау кілтінің өсу дискреті ұзындығы 1-ден 16 битке дейінгі интервалда мүмкін болады. Бұл интервал үздіксіз мәліметтермен жұмыс істеудің есептеу қиындығының баяу өсуіне сәйкес келеді.

Түрлендіргіш жағдайының көп өлшемді энтропиясының $n=16$ нүктесінде биометрия-коды өзінің қасиеттерін өзгертеді және интегралдық шабуылдар жұмыс істей бастайды. Интегралдық шабуылдар статистикалық зерттеулерге арналған қолжетімді биометрия-код ұзын болған сайын тиімдірек болады.

2.3 Бетпе-бет келетін байланыстары бар нейрондарды итерациялық үйретуге жиі қайту арқылы шифрлау тұрақтылығын жоғарылату. Бүгінгі күні нейрожелілік контейнерге қауіпті шабуылдардың бірі Маршалко шабуылы болып табылады. Үлкен жасанды нейрондық желілерді үйретудің жылдам алгоритмдері – $\mu(E(v_i), \sigma(v_i), \sigma(\xi_i))$ нейрондардың салмақтық коэффициенттерінің детерминделген есептеулерін құруда шабуыл пайда болады. Дәл осы себепті үйрету алгоритмдері жылдам және осы себептен Маршалко шабуылы орын алуы мүмкін.

Егер біз үлкен нейрожеліні үйрету тәсілін өзгертсек және МЕСТ Р 52633.5-те жазылған есептеулерден кейін олардың итерациялық дәлдеулерін қолдансақ, онда біз қалыпты шешімдер аймағында қалыптыға жақын жақсы және нашарлау болатын жуық шешімдердің жиынтығын табамыз. Мұнда шешімдердің шырғалану қаупі жағымсыз рөл емес, оңтайлы рөл атқарады. «Өзім» үлгілерінің аз сандарының ішкі шуылдарынан барлық итерациялық үйрету алгоритмдерін, реттелетін параметрлерінің әрқайсысы бойынша сапа көрсеткіші туындысын есептеу кезінде жіберілген өз қатесінің әсерін минималды ете отырып, кейбір көп өлшемді беттер бойынша флюктуирлейді. Итерациялық үйрету және нейрондардың кіріс саны көп болғанында нейрондардың салмақтық коэффициенттері шуылының табиғи үрдісі пайда болады. Ол 4-суретінде көрсетілген [13, с.66].



Сурет 4 – Бір нейронды итерациялық үйрету процедурасы тұрақтылығының төмендеуі

Қ.И.Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университетінің зертханасында жүргізілген зерттеулер, үйретілген нейронның итерациялық алгоритмі арқылы табылған барлық шешімдері арасында бір-біріне өзара дәл келетін салмақ коэффициенттері жоқтығын көрсетті.

Оның үстіне осы шешімдердің 1% дан 15%-ға дейінгі салмақтық коэффициенттері түрлі таңбаларға ие болады. Бұл жағдайда Маршалко шабуылы қабілетсіз болады, яғни итерациялық үйретуді бірнеше рет іске қосу және үйретуге дейін нейронның ортақ байланыстары бар салмақтық коэффициенттерінде МЕСТ Р 52633.5-2011 үйрету алгоритмінің таңбаларына қайшы келетін шешімді табуға болады.

Әрине, ішінара итерациялық үйрету алгоритмі немесе нейрондық желіні толық итерациялық үйрету алгоритмі үйрету үрдісін айтарлықтай баяулатады, бірақ сонымен қатар, нейрондардың артық байланыстарына төнетін шабуылдан тиімді қорғаныс туындайды.

Мұндағы тағы да бір әзірленген алгоритм - мәліметтерді мәжбүрлеп бұзудың жылдам алгоритмі. Бұл алгоритм бойынша нейрондардың жалпы байланысының 50%-ы шағын (үлкен емес) болады және олардың таңбасы өзгереді. Әрі қарай үйрету кезінде бүлінген байланыстар

өзгермейді. Бұл нейронды алғаш үйретуден соң керек нәтижені алуды қамтамасыз етеді. Мұнда үйретудің итерациялық алгоритмі жұмыс істеу үшін нейрондардың басқа кірістерінің салмағын кездейсоқ түрде 15%-ға дейін өзгертеді (таңбасын өзгертпей) және осыдан кейін ғана үйретудің итерациялық алгоритмін қолдана отырып, шамамен алғанда 100-200 итерациядан кейін үйретудің алдын жоғалтылған сапасын қайтарып алуға болады. Бұдан өзге жаңа шешімдердің шамамен алғанда 60%-ы итерациялық емес түрде МЕСТ Р 52633.5-2011 бойынша алынған шешімге қарағанда жақсы болып шығады.

Жүргізілген зерттеулер нәтижесінде болар-болмас бүлінетін биометриялық кодтың нейро-желілік түрлендіргішін итерациялық емес үйретудің гибриді нұсқасы және оларды әрі қарай үйрету Маршалко шабуылына өте табанды, барынша сапалы шешім (тойтарыс) беретіні дәлелденді.

Қорытынды. Айта кететін жайт, тек қана техникалық құралдармен жүйені тиімді қорғау мүмкін емес яғни ұйымдастырушылық, заңдылық, физикалық және техникалық кешен қажет. Осы мақала шеңберінде біз ақпараттарды нейрожелілік биометриялық қорғау құралдарына төнетін қауіптерге қарсы тұру әдістері қарастырылды. Олардың әрқайсысы тәжірибеде Қ.И.Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университетінің және Пенза мемлекеттік университетінің зертханаларында қарастырылып, ұсынылып отыр.

ӘДЕБИЕТ

- [1] Болл Р., Коннел Дж.Х., Панканти Ш.Р., Налини К., Сеньор Э.У. Руководство по биометрии. –М.: Техносфера, 2007. -368 с.
- [2] Иванов А.И., Сорокин И.А. Автоматическая система идентификации личности по динамике подписи. //Новые промышленные технологии. -1993. -№ 6. –С. 56-63.
- [3] Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. - Пенза: Изд-во ПГУ, 2000. -188 с.
- [4] Рыбченко Д.Е., Иванов А.И. Анализ клавиатурного почерка аппаратом нечетких множеств для целей ограничения доступа и аудита. // Специальная техника средств связи. Серия. Системы, сети и технические средства конфиденциальной связи. -Пенза: ПНИЭИ, 1996.-С.116 -119.
- [5] Атал Б. Автоматическое опознавание дикторов по голосам. // ТИИЭР. -1976. -Т. 64, №4. -С. 48-66.
- [6] Розенберг А. Автоматическая верификация диктора: Обзор. // ТИИЭР. -1976. -Т. 64, №4. -С. 66-79.
- [7] Volchihin V., Akhmetov B. S., Ivanov A., Malygin A., Kartbayev T.S. Highly Reliable Human-Being Personality's Multi-Biometric Authentication to Support Citizens Interaction // Global Journal on Technology, – North America, 2013. Available at: <http://www.world-education-center.org/index.php/P-ITCS/article/view/1728/1524>.
- [8] Akhmetov B., Kartbayev T., Doszhanova A., Ivanov A., Malygin A. Biometric technology in securing the Internet using large neural network technology // World Academy of science, Engineering and technology, -Singapore. 2013, -Iss.79, -P. 129-138
- [9] Ахметов Б.С., Досжанова А.А., Иванов А.И., Картаев Т.С., Малыгин А.Ю. Технология биометрического обезличивания электронных историй болезней пациентов медицинских учреждений // Вестник КазНТУ. -Алматы. 2013. - № 3(97). - С. 186-190.
- [10] Akhmetov B.S., Ivanov A.I., Kartbaev T.S., Malygin A.U., Mukapil K. Biometric Dynamic Personality Authentication in Open Information Space // International Journal of Computer Technology and Applications. -India, 2013.-Vol. 4, Issue 5. -P. 846-855.
- [11] Ахметов Б.С., Алисов В.А., Вятчанин С.Е., Сауанова К.Т. Нейросетевая мультибиометрическая аутентификация личности гражданина в системе электронного правительства. // Сборник трудов Международного симпозиума «Надежность и качество – 2012». -Пенза: Изд-во ПГУ, 2012. –Т. 1. – С. 227-229.
- [12] Фунтиков В.А., Иванов А.И., Федулаев В.В., Ефимов О.В. Дружественный биометрико-нейросетевой формирователь ЭЦП служащего с высоконадежной степенью авторизации //Специальная техника средств связи / Электронная версия на сайте <http://refdb.ru/look/1872689.html>.
- [13] Волчихин В.И., Иванов А.И., Назаров И.Г., Фунтиков В.А., Язов Ю.К. Нейросетевая защита персональных биометрических данных. -М.: Радиотехника, 2012. -160 с.
- [14] Пат. RU 2346397. Способ защиты персональных данных биометрической идентификации и аутентификации, / Иванов А.И., Фунтиков В.А., Ефимов О.В.; опубл. 10.02.2009, Бюл. №4
- [15] Фунтиков В.А., Назаров И.Г., Бурушкин А.А. Национальные стандарты России: конфиденциальность персональных биометрических данных. // Стандарты и качество. -2010. -№ 7. -С. 28-33.

REFERENCES

- [1] Boll R., Konnel Dzh.H., Pankanti Sh.R., Nalini K., Sen'or Je.U. Rukovodstvo po biometrii. –M.: Tehnosfera, 2007. - 368 s.
- [2] Ivanov A.I., Sorokin I.A. Avtomaticheskaja sistema identifikacii lichnosti po dinamike podpisi. // Novyye promyshlennyye tehnologii. -1993. -№ 6. –S. 56-63.

- [3] Ivanov A.I. Biometricheskaja identifikacija lichnosti po dinamike podsoznatel'nyh dvizhenij. - Penza: Izd-vo PGU, 2000. -188 s.
- [4] Rybchenko D.E., Ivanov A.I. Analiz klaviaturnogo pocherka apparatom nechetkih mnozhestv dlja celej ogranichenija dostupa i audita. // Special'naja tehnika sredstv svjazi. Serija. Sistemy, seti i tehnicheckie sredstva konfidencial'noj svjazi. -Penza: PNIJeI, 1996. -S.116 -119.
- [5] Atal B. Avtomaticheskoe opoznavanie diktorov po golosam. // TIJeR. -1976. -T. 64, №4. -S. 48-66.
- [6] Rozenberg A. Avtomaticheskaja verifikacija diktora: Obzor. // TIJeR. -1976. -T. 64, №4. -S. 66-79.
- [7] Volchihin V., Akhmetov B. S., Ivanov A., Malygin A., Kartbayev T.S. Highly Reliable Human-Being Personality's Multi-Biometric Authentication to Support Citizens Interaction // Global Journal on Technology, – North America, 2013. Available at: <http://www.world-education-center.org/index.php/P-ITCS/article/view/1728/1524>.
- [8] Akhmetov B., Kartbayev T., Doszhanova A., Ivanov A., Malygin A. Biometric technology in securing the Internet using large neural network technology // World Academy of science, Engineering and technology, -Singapore. 2013, -Iss.79, -P. 129-138
- [9] Ahmetov B.S., Doszhanova A.A., Ivanov A.I., Kartbaev T.S., Malygin A.Ju. Tehnologija biometricheskogo obezlicivaniya jelektronnyh istorij boleznj pacientov medicinskih uchrezhdenij // Vestnik KazNTU. -Almaty. 2013. - № 3(97). - S. 186-190.
- [10] Akhmetov B.S., Ivanov A.I., Kartbaev T.S., Malygin A.U., Mukapil K. Biometric Dynamic Personality Authentication in Open Information Space // International Journal of Computer Technology and Applications. -India, 2013. -Vol. 4, Issue 5. -P. 846-855.
- [11] Ahmetov B.S., Alisov V.A., Vjatchanin S.E., Sauanova K.T. Nejrosetevaja mul'tibiometricheskaja autentifikacija lichnosti grazhdanina v sisteme jelektronnogo pravitel'stva. // Sbornik trudov Mezhdunarodnogo simpoziuma «Nadezhnost' i kachestvo – 2012». -Penza: Izd-vo PGU, 2012. –T. 1. – S. 227-229.
- [12] Funtikov V.A., Ivanov A.I., Fedulaev V.V., Efimov O.V. Druzhestvennyj biometriko-nejrosetevoj formirovatel' JeCP sluzhashhego s vysokonadezhnoj stepen'juavtorizacii // Special'naja tehnika sredstv svjazi / Jelektronnaja versija na sajte <http://refdb.ru/look/1872689.html>.
- [13] Volchihin V.I., Ivanov A.I., Nazarov I.G., Funtikov V.A., Jazov Ju.K. Nejrosetevaja zashhita personal'nyh biometricheskikh dannyh. -M.: Radiotekhnika, 2012. -160 s.
- [14] Pat. RU 2346397. Sposob zashhity personal'nyh dannyh biometricheskoi identifikacii i autentifikacii, / Ivanov A.I., Funtikov V.A., Efimov O.V.; opubl. 10.02.2009, Bjul. №4
- [15] Funtikov V.A., Nazarov I.G., Burushkin A.A. Nacional'nye standarty Rossii: konfidencial'nost' personal'nyh biometricheskikh dannyh. // Standarty i kachestvo. -2010. -№ 7. -S. 28-33.

Б.С.Ахметов, Т.С.Картбаев, А.А.Досжанова

Казахский национальный медицинский университет имени С.Д.Асфендиярова, Алматы

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ СРЕДСТВАМ БИОМЕТРИКО-НЕЙРОСЕТЕВОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. На сегодняшний день недостаточно защищать систему только с помощью технического обеспечения: для надежности защиты надо обеспечить организационный, правовой, физический и технический комплекс мер. В данной статье рассматриваются методы противодействия угрозам средств биометрико-нейросетевой защиты информации. Каждый метод рассмотрен на практике в лабораториях Казахского национального исследовательского технического университета имени К.И. Сатпаева и Пензенского государственного университета.

Ключевые слова: информационная безопасность, биометрия, нейросети, аутентификация, угрозы, защита информации.

Сведения об авторах:

Ахметов Бахытжан Сражатдинович – доктор технических наук, профессор Казахского национального исследовательского технического университета имени К.И.Сатпаева, академик Международной академии информатизации;

Картбаев Тимур Саатдинович – PhD, заместитель директора по развитию информационных технологий Казахского национального медицинского университета имени С.Д.Асфендиярова, академик Международной академии информатизации;

Досжанова Алия Амантаевна – PhD, заведующая кафедрой информационных технологий Казахского государственного женского педагогического университета, академик Международной академии информатизации.

МАЗМҰНЫ
Техникалық ғылымдар

Азаматов Б.Н., Ожикенев Қ.А., Азаматова Ж.Қ. ЖЭС гидравликалық күлжою жүйесінде геометриясы басқарылатын гидроциклондар батареясын автоматты басқару 5

Қоғамдық ғылымдар

Қалдыбай Қ.Қ., Пазылова Қ.А. Агрессия концепциясын теориялық тұрғыдан әлеуметтік-психологиялық талдау.... 14

Техникалық ғылымдар

Сахметова Г.Е., Бренер А.М., Калдыбаева Б.М., Абильмағжанов А.З. Биогазды өндіру үшін қондырғыларды жобалау кезінде ауқымды өтпе мәселелерінің режимдік аспектілері..... 21

Ахметов Б.С., Қартбаев Т.С., Досжанова А.А. Ақпараттарды нейрожелілік биометриялық қорғау құралдарына төнетін қауіпке қарсы тұру әдістері..... 28

Мукажанов Н.К., Кисанов А. М., Мусапирова Г.Д. Кеңістіктік объектілер образын тану бойынша зерттеу..... 35

Найзабеков А.Б., Волокитина И.Е. Мыс микроқұрылымның эволюциясына ТКББ әсерін зерттеу 41

Цекич Н. Қазіргі заманғы экологиялық қалалық сәулет кешенін жобалау..... 48

Ожикенов Қ.Ә., Рахметова П.М., Ожикен А.Қ. Манипуляциялық роботты адаптивті басқару жүйесіндегі динамикалық үрдістерді бейімді тұрақтандыру..... 58

Ракишев Б.Р., Прокопенко В.И., Череп А.Ю., Ковров А.С. Топты карьерлер жұмысы кезінде бұзылған жер бетін жөндеудің ерекшеліктері..... 66

Аграрлық ғылымдар

Баймұқанов Д.А., Баймұқанов А., Юлдашбаев Ю.А., Исхан К.Ж., Алиханов О., Дошанов Д. F₄ сүлесіндегі қазак дромедар түйесінің өнімділігі..... 74

Химия

Суербаев Х.А., Құдайбергенов Н.Ж., Елібай К.Б. Терминалды олефиндерді палладий фосфин комплекстері қатысында көмітек монооксидіжәне спирттермен карбонилдеу 85

Биология

Абайлдаев А.О., Неупокоева А.С., Рахымғошин М.Б., Ходаева А.С., Ботбаев Д.М., Аширбеков Е.Е., Куланбаев Е.М., Хансеитова А.К., Балмуханов Т.С., Айтхожина Н.А. Қазақстан популяциясындағы сүт безі ісігі диагнозына шалдыққан наукастардың *LSP1* гені өзгеріштігінің ассоциациясы..... 108

Қоғамдық ғылымдар

Кишибекова Г. К., Омарханова Ж. М. Қазақстан республикасы ауыл шаруашылығы дамуын қаржымен қамтамасыз ету..... 115

Абдулина Г.А., Сейтхамзина Г. Ж. Заманауи кәсіпорындардың әлеуметтік даму проблемалары 126

Абылкасимова Ж.А., Алибаева М.М., Орынбекова Г.А., Ракишев А.А. Қазіргі жағдайдағы Қазақстанның агроөнеркәсіп кешені субъектілерінің экономикалық интеграциясы..... 136

Азатбек Т.А., Байтеңізев Д.Т. Ғылыми білім жүйесіндегі өзін-өзі жұмыспен қамту 142

Аюпова З.К., Құсайынов Д.Ө. Қазақстан республикасының құқықтық саясаты мемлекеттілікті нығайтудың басты механизмі ретінде..... 150

Рамазанов А.А., Кажмуратова А.К., Тымбаева Ж.М. Қазақстан республикасының мұнай нарығының экономикалық өлшемі 157

Сембиева Л.М., Бекбенбетова Б.Б., Бейсенова Л.З. ЕЭҚ-тың Қазақстан кредиттік жүйесі проблемалары мен Келешегі..... 167

Удербаета С.К. Орынбор ғылыми мұрағат комиссиясының «Еңбектер» жинағындығы орталық азияның көшпелі халықтарының тарихы..... 177

Болтаева А.А. Мемлекеттің бизнестің әлеуметтік жауапкершілігін жүзеге асырудағы ролі 189

СОДЕРЖАНИЕ

Технические науки	
<i>Азаматов Б.Н., Ожикенев К.А., Азаматова Ж.К.</i> АСУбатарей гидроциклонов с управляемой геометрией в системе ГЗУ ТЭС.....	5
Общественные науки	
<i>Калдыбай К.К., Пазылова К. А.</i> Социально-психологической анализ концепции агрессии.....	14
Технические науки	
<i>Сахметова Г.Е., Бренер А.М., Калдыбаева Б.М., Абиьлмагжанов А.З.</i> Режимные аспекты проблемы масштабного перехода при проектировании установок для производства биогаза.....	21
<i>Ахметов Б.С., Картбаев Т.С., Досжанова А.А.</i> Методы противодействия средствам биометрико-нейросетевой защиты информации.....	28
<i>Мукажанов Н.К., Кисапов А. М., Мусатирова Г.Д.</i> Исследования по распознаванию образов пространственных объектов.....	35
<i>Найзабеков А.Б., Волокитина И.Е.</i> Исследование влияния круп на эволюцию микроструктуры меди.....	41
<i>Цекич Н.</i> Комплексное проектирование в современной экологической городской архитектуре.....	48
<i>Ожикенев К.А., Рахметова П.М., Ожикен А.К.</i> Адаптивная стабилизация динамических процессов в системе управления манипуляционным роботом.....	59
<i>Ракишев Б.Р., Прокопенко В.И., Череп А.Ю., Ковров А.С.</i> Особенности горнотехнической рекультивации нарушенных земель при разработке группы карьеров	66
Аграрные науки	
<i>Баймуканов Д. А., Баймуканов А., Юлдашбаев Ю. А., Исхан К., Алиханов О., Дошанов Д.</i> Продуктивность верблюдов дромедаров казахского типа F ₄	74
Химия	
<i>Суербаяв Х.А., Кудайбергенов Н.Ж., Елибай К.Б.</i> Карбонилирование терминальных олефинов монооксидом углерода и спиртами в присутствии фосфиновых комплексов палладия.....	85
Биология	
<i>Абайлдаев А.О., Неупокоева А.С., Рахымгожин М.Б., Ходаева А.С., Ботбаев Д.М., Аширбеков Е.Е., Куланбаев Е.М., Хансеитова А.К., Балмуханов Т.С., Айтхожина Н.А.</i> Ассоциация вариабельности в гене <i>LSP1U</i> пациентов с диагнозом рак молочной железы в популяциях казахстана.....	108
Общественные науки	
<i>Кишибекова Г. К., Омарханова Ж. М.</i> Финансовое обеспечение развития сельского хозяйства республики Казахстан.....	115
<i>Абдулина Г.А., Сейтхамзина Г. Ж.</i> Проблемы социального развития современных компаний.....	126
<i>Абылкасимова Ж.А., Алибаева М.М., Орынбекова Г.А., Ракишев А.А.</i> Экономическая интеграция субъектов агропромышленного комплекса Казахстана в современных условиях.....	136
<i>Азатбек Т.А., Байтенизов Д.Т.</i> Самозанятость в системе научного знания.....	142
<i>Аюпова З.К., Кусаинов Д.У.</i> Правовая политика республики Казахстан как важный механизм укрепления государственности.....	150
<i>Рамазанов А.А., Кажмуратова А.К., Тымбаева Ж.М.</i> Экономическое измерение нефтяного рынка Республики Казахстан	157
<i>Сембиева Л.М., Бекбенбетова Б.Б., Бейсенова Л.З.</i> Проблемы и перспективы развития кредитной системы Казахстана в рамках ЕАЭС.....	167
<i>Удербаяева С.К.</i> Отражение истории кочевых народов Центральной Азии в «Трудах» Оренбургской ученой архивной комиссии.....	177
<i>Болтаева А.А.</i> Роль государства в реализации социальной ответственности бизнеса.....	189

CONTENT

Technical sciences	
<i>Azamatov B.N., Ozhikenov K.A., Azamatova Zh. K.</i> ACS of the set of hydrocyclones with a variable geometry in the system of HAR TPP	5
Social Sciences	
<i>Kaldybay K.K., Pazylova K.A.</i> Socio-psychological analysis of the concept of aggression.....	14
Technical sciences	
<i>Sakhmetova G.E., Brener A.M., Kaldybaeva B.M., Abilmagzhanov A.Zh.</i> "Regime aspects of the scale -up problem while designing installations for biogas production	21
<i>Akhmetov B.S., Kartbayev T.S., Doszhanova A.A.</i> Methods of counteraction to means of biometric-neural network protection of information.....	28
<i>Mukazhanov N.K., Kisapov A.M., Musapirova G.D.</i> Studies on the recognition of images of spatial objects.....	35
<i>Nayzabekov A.B., Volokitina I.E.</i> Research of the influence of the ecap on the evolution of the microstructure of copper.....	41
<i>Cekic N.</i> Integrated design in contemporary ecological urban architecture.....	48
<i>Ozhikenov K.A., Rakhmetova P.M., Ozhiken A.K.</i> Adaptive stabilization of dynamic processes in the control system of a manipulation robot.....	59
<i>Rakishev B., Prokopenko V., Cherep A., Kovrov A.</i> Features of mining-technical recultivation of disturbed lands during development of mines.....	66
Agricultural science	
<i>Baimukanov D.A., Baimukanov A., Yuldashbaev Yu. A., Ishan K., Alikhanov O., Doshanov D.</i> Productivity of the camelsdromedary of kazakh type F ₄	74
Chemistry	
<i>Suerbaev Kh.A., Kudaibergenov N.Zh., Yelibay K.B.</i> Carbonylation of terminal olefines by carbon monoxide and alcohols in the presence of palladium phosphin complexes.....	85
Biology	
<i>Abaildayev A.O., Neupokoeva A.S., Rahymgozhin M.B., Khodayeva A.Y., Botbayev D.M., Ashirbekov Y.Y., Kulanbayev E.M., Khanseitova A.K., Balmuhanov T.S., Aitkhozhina N.A.</i> Association of variability of <i>ISP1</i> gene in patients with breast cancer from populations of Kazakhstan	108
Social Sciences	
<i>Kishibekova G. K., Omarkhanova Zh. M.</i> Financial security of development of agriculture of the republic of Kazakhstan.....	115
<i>Abdulina G.A., Seitkhamzina G.Zh.</i> Problems of social development of modern companies.....	126
<i>Abylkassimova Zh., Alibaeva M., Orynbekova G., Rakishev A.</i> Economic integration of subjects of the agro-industrial complex of Kazakhstan in modern conditions.....	136
<i>Azatbek T.A., Baitenizov D.T.</i> Self-employment in the system of scientific knowledge.....	142
<i>Ayupova Z.K., Kussainov D.U.</i> Legal policy of the republic of Kazakhstan as important mechanism of strengthening of statehood.....	150
<i>Ramazanov A., Kazhuratova A., Tymbaeva Zh.</i> Economic measurement of the oil market of the Republic of Kazakhstan.....	157
<i>Sembiyeva L.M., Bekbenbetova B.B., Beisenova L.Z.</i> Problems and prospects for the development of the credit system of Kazakhstan within the framework of the EEU.....	167
<i>Uderbaeva C.K.</i> Reflection of the history of the nomadic peoples of Central Asia in the "Proceedings" of the Orenburg archival scientific commission.....	177
<i>Boltaeva A.A.</i> The role of the state in the implementation of social responsibility of business.....	189

Publication Ethics and Publication Malpractice in the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethical guidelines for journal publication see <http://www.elsevier.com/publishingethics> and <http://www.elsevier.com/journal-authors/ethics>.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the work described has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see <http://www.elsevier.com/postingpolicy>), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the originality detection service Cross Check <http://www.elsevier.com/editors/plagdetect>.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www.nauka-nanrk.kz

ISSN 2518-1483 (Online), ISSN 2224-5227 (Print)

<http://www.reports-science.kz/index.php/ru/>

Редакторы *М. С. Ахметова, Д. С. Аленов, Т.А. Апендиев*
Верстка на компьютере *А.М. Кульгинбаевой*

Подписано в печать 15.08.2017.

Формат 60x881/8. Бумага офсетная. Печать – ризограф.
12,3 п.л. Тираж 2000. Заказ 4.